

TOPOLOGY OF DIOPHANTINE SETS: REMARKS ON MAZUR'S CONJECTURES

GUNTHER CORNELISSEN AND KARIM ZAHIDI

ABSTRACT. We show that Mazur's conjecture on the real topology of rational points on varieties implies that there is no *diophantine model* of the rational integers \mathbf{Z} in the rational numbers \mathbf{Q} , i.e., there is no diophantine set D in some cartesian power \mathbf{Q}^i such that there exist two binary relations S, P on D whose graphs are diophantine in \mathbf{Q}^{3i} (via the inclusion $D^3 \subset \mathbf{Q}^{3i}$), and such that for two specific elements $d_0, d_1 \in D$ the structure (D, S, P, d_0, d_1) is a model for integer arithmetic $(\mathbf{Z}, +, \cdot, 0, 1)$.

Using a construction of Pheidas, we give a counterexample to the analogue of Mazur's conjecture over a global function field, and prove that there is a diophantine model of the polynomial ring over a finite field in the ring of rational functions over a finite field.

1. INTRODUCTION

One of the main themes in model theory is to understand the structure of definable sets: given a first-order language L and an L -structure M , describe the L -definable subsets of M^n for various $n \in \mathbf{Z}_{>0}$. Here, a set $S \subset M^n$ is called L -definable if there exists an L -formula $\psi(\mathbf{x})$ with free variables $\mathbf{x} = (x_1, \dots, x_n)$ such that for any $\mathbf{a} \in M^n$, $\mathbf{a} \in S \iff M \models \psi(\mathbf{a})$. A set is called existentially definable (respectively, positive existentially, or diophantine) if $\psi(\mathbf{x})$ can be taken to be $\exists \mathbf{b} \phi(\mathbf{x}, \mathbf{b})$, with ϕ quantifier-free (respectively, quantifier- and negation-free, or atomic).

The natural geometric examples of such structures arise as in the following definition:

Definition 1.1. If R is a commutative ring with unit, it admits a natural interpretation for any first order language L of the form $L_R = (+, \cdot, =, c_i)$ where c_i are primary predicates ("constants"), less in number than $|R|$. We call L_R a *ring language*. We define $L_{\mathbf{Z}} = (+, \cdot, 0, 1)$ and $L_t = (+, \cdot, 0, 1, t)$ for any $t \in R$.

Example 1.2. (Tarski, cf. [9], pp. 202–206) (a) An algebraically closed field k admits elimination of quantifiers in the language $L_{\mathbf{Z}}$. Hence any $L_{\mathbf{Z}}$ -definable subset in k^n is a boolean combination of sets defined by an equation. Thus, the definable sets for an algebraically closed field are exactly the classical sets of algebraic geometry – one deduces for example that the only definable subsets of k are finite or cofinite, a fact which at first sight seems not so obvious.

(b) The field of real numbers \mathbf{R} admits elimination of quantifiers in the language $L_{\geq} = (0, 1, +, \cdot, \geq)$ of ordered fields. Hence every definable set in \mathbf{R}^n is a boolean combination of semi-algebraic sets (i.e., solution sets to systems of equations of the

1991 *Mathematics Subject Classification.* 03D35, 14G05.

The first author is Post-doctoral fellow of the Fund for Scientific Research - Flanders (FWO).

form $f(\mathbf{x}) = 0 \wedge g(\mathbf{x}) \geq 0$). This gives a nice description of the definable subsets of \mathbf{R} : they are finite unions of intervals.

(c) More examples in the same vein exist, e.g., a description of definable sets over p -adic fields ([12], [5]), or generalization of (\mathbf{R}, L_{\geq}) via o-minimal expansions.

(d) To give an example with a different language, existentially definable sets of \mathbf{Z} in the language $(0, 1, +, |)$ are unions of arithmetic progressions (a result of Lipshitz [11]).

The moral is that if the (existentially) definable sets for such M have a sufficiently easy description, then the first-order (respectively, existential) theory of M is decidable – this is the case in the above examples. Conversely, if definable sets are combinatorially complicated, one expects the corresponding theory to be undecidable.

Example 1.3. (a) Consider the rational integers $(\mathbf{Z}, L_{\mathbf{Z}})$. It is impossible to describe the $L_{\mathbf{Z}}$ -definable sets of \mathbf{Z} in terms of “classical” sets (e.g., finite sets, arithmetic progressions, ...). Eventually, this leads to the undecidability of the full theory of $(\mathbf{Z}, L_{\mathbf{Z}})$.

(b) The celebrated theorem of Davis, Matijasevich, Putnam and Robinson describes the existentially definable sets of \mathbf{Z} : they are exactly the recursively enumerable sets, whose complexity outranges by far that of decidable (hence, certainly, of computable) sets – and the undecidability of the existential theory of $(\mathbf{Z}, L_{\mathbf{Z}})$ follows.

This maxim, the interplay between (un)decidability and definable sets, applies in particular to the field $(\mathbf{Q}, L_{\mathbf{Z}})$ of rational numbers. The field structure of \mathbf{Q} admits the same kind of “wild” definable sets as the integers; this follows from J. Robinson’s theorem that \mathbf{Z} is a definable subset of \mathbf{Q} ([21], theorem 3.1). The question whether the same can happen if we restrict to the existentially definable sets is still open.

In the next paragraph, we will present a conjecture by Mazur, which – although it does not characterize the existentially definable sets of \mathbf{Q} – poses severe restrictions on their real topological structure. In the subsequent section, we prove that this conjecture implies there is no “diophantine model” (cf. *infra*) of $(\mathbf{Z}, L_{\mathbf{Z}})$ in $(\mathbf{Q}, L_{\mathbf{Z}})$ – this generalizes Mazur’s observation that his conjecture implies that \mathbf{Z} is not an $L_{\mathbf{Z}}$ -diophantine subset of \mathbf{Q} . In particular, any proof of the diophantine undecidability of \mathbf{Q} “along traditional lines” fails if Mazur’s conjecture is true. In the final paragraph, we comment upon a non-archimedean version of this conjecture. Though most of these observations are folklore, they do not seem to have been written down previously.

2. MAZUR’S CONJECTURES

In [14], [15] and [16], Barry Mazur has proposed and discussed several conjectures and questions about the behaviour of the set of \mathbf{Q} -rational points of a variety over \mathbf{Q} under taking topological closure w.r.t. some metric induced by a valuation on \mathbf{Q} . The conjecture that we will concentrate upon (the weakest) is the following:

Conjecture 2.1. (Mazur [16], Conjecture 3) *For any variety V over \mathbf{Q} , the (real) topological closure of $V(\mathbf{Q})$ in $V(\mathbf{R})$ has only a finite number of real topological components.*

There is some evidence for this conjecture, especially for such V which possess special geometric properties (mostly related to the canonical class of V) – and no counterexample to it is known. Also observe that, with \mathbf{Q} replaced by \mathbf{R} in 2.1, the “conjecture” says that a real variety has only finitely many real connected components. This holds true; it could be deduced from Tarski’s results – there is even an explicit bound on the betti numbers of $V(\mathbf{R})$, the so-called Milnor-Thom theorem (cf. [17]).

Example 2.2. (a) Conjecture 2.1 is true for curves V . One can assume V to be projective and non-singular. The case where V has genus $g \geq 2$ is settled by Faltings’s theorem, which says that $V(\mathbf{Q})$ is a finite set ([6]). If V has genus 0, then either $V(\mathbf{Q})$ is empty, or V is \mathbf{Q} -birational to \mathbf{A}^1 , and $\mathbf{A}^1(\mathbf{Q})$ is topologically dense in $\mathbf{A}^1(\mathbf{R})$. Finally, assume that V has genus 1. It is known that $V(\mathbf{R})$ is isomorphic to the “circle group” \mathbf{R}/\mathbf{Z} or to $\mathbf{R}/\mathbf{Z} \times \mathbf{Z}/2$ (see [22], V). Every proper closed subgroup of the circle group is finite (see [8], theorem 1.34). Hence, if $V(\mathbf{Q})$ is not finite, then it is dense in every component of $V(\mathbf{R})$ that it intersects.

(b) To provide a higher dimensional example, let V be a variety satisfying weak approximation (i.e., such that $V(\mathbf{Q}) \hookrightarrow \prod V(\mathbf{Q}_p)$ is dense). Then the conjecture holds true for V . This holds, e.g., if V is a smooth complete intersection of two quadrics in projective space of dimension at least 5 (cf. [14]).

Remark 2.3. Mazur has made even stronger conjectures, some of which had to be slightly modified, due to the construction of a counterexample by Colliot-Thélène, Skorobogatov and Swinnerton-Dyer ([1]). For an extensive (unsurpassable) exposition and more examples, we refer to the original sources [14], [15] and [16]. We will concentrate on the model-theoretical aspects of the conjectures, which are already present in 2.1 – but let the reader be warned about making too bold generalizations of 2.1. A non-archimedean version will be considered in the last paragraph of this paper.

Remark 2.4. The $(\mathbf{Q}, L_{\mathbf{Z}})$ -existentially definable subsets, in the sense of the introduction, are precisely images of projections from $V(\mathbf{Q})$ to affine space $\mathbf{A}_{\mathbf{Q}}^n$ for various V and n .

A more model-theoretic conjecture would be that *the real topological closure of a $(\mathbf{Q}, L_{\mathbf{Z}})$ -existentially definable set is an (\mathbf{R}, L_{\geq}) -definable set* (i.e., a semi-algebraic set). This implies 2.1, since a semi-algebraic set has only finitely many components.

We do not know whether conjecture 2.1 is equivalent to this statement. Note that J. Robinson’s argument (in [21]) shows that it is wrong when the word “existentially” is erased.

3. DIOPHANTINE MODELS OF \mathbf{Z} IN \mathbf{Q}

Mazur has observed that conjecture 2.1 implies that \mathbf{Z} is not diophantine in \mathbf{Q} in the language $L_{\mathbf{Z}}$; indeed, if \mathbf{Z} would arise as the projection of $V(\mathbf{Q})$ for some variety V , then since \mathbf{Z} has infinitely many real components and the projection is continuous, the same would hold for $V(\mathbf{R})$.

However, many proofs of the undecidability of the diophantine theory of structures (R, L_R) as in (1.1) do not give that \mathbf{Z} is a diophantine *subset* of R , but rather produce a *diophantine model* of $(\mathbf{Z}, L_{\mathbf{Z}})$ in (R, L_R) , in the sense of the following definition:

Definition 3.1. A model (M, L, ϕ) is a triple consisting of a first order language L which consists of i -ary predicates $\{P_{i,\alpha}\}$, a set M and an interpretation ϕ of L in M (we will often leave out ϕ of the notation). Note that any cartesian power M^k , ($k \geq 1$) is likewise a model for L via “diagonal interpretation”.

We say that a model $(M', L' = \{P'_{i,\alpha}\}, \phi')$ admits a *diophantine model* in (M, L, ϕ) if there exists a set-theoretical bijection between M' and a subset of some cartesian power M^k ($k \geq 1$), such that the image is diophantine, and such that the induced inclusions $\phi'(P'_{i,\alpha}) \subseteq M^{ik}$ are diophantine.

A similar notion of (*positive*) *existential model* exists.

Example 3.2. (a) If (M^2, L) admits a diophantine model in (M, L) , then the latter structure is said to admit *diophantine storing* (cf. [2]). This is true, for example, for $(\mathbf{Z}, L_{\mathbf{Z}})$. For non-algebraically closed rings (R, L_R) admitting diophantine storing, one can always choose $k = 1$ in the above definition. For if (M', L', ϕ') admits a diophantine model in (R^2, L_R) and (R, L_R) admits diophantine storing, then (M', L', ϕ') admits a diophantine model in (R, L_R) (since conjunctions of diophantine formulas are again diophantine if the quotient field of R is not algebraically closed – cf. [2], §3).

(b) Typically, diophantine models of the integers $(\mathbf{Z}, L_{\mathbf{Z}})$ in ring languages (R, L_R) arise in the following way: a commutative algebraic group G (e.g., the multiplicative group of a quadratic ring, or an elliptic curve) is assumed to have rank one over R , and the set \mathbf{Z} has a diophantine model as the R -rational points $G(R)$ of G – the relation “addition” is automatically mapped to a diophantine subset of $G^3(R)$, since the group law on G is a morphism. The most problematic point is defining the relation “multiplication”. For an example, consider the proof that $(\mathbf{Z}, L_{\mathbf{Z}})$ admits a diophantine model in $(R := S[t], L_t)$ for any commutative unitary domain S of characteristic zero, see Denef [4]. He takes for G the torus $\mathbf{G}_{m,R[\sqrt{\Delta}]}$ of discriminant $\Delta = t^2 - 1$, which is non-split over R ; $G(R)$ has rank one: any R -point is given by a solution (x_n, y_n) to the Pell-equation $X^2 - \Delta Y^2 = 1$ (i.e., a power $u^n = x_n + y_n \sqrt{\Delta}$ of the fundamental unit $u = t + \sqrt{\Delta}$). Multiplication $(x_r, y_r) \cdot (x_s, y_s) = (x_n, y_n)$ is defined by saying that $f := y_n - y_r \cdot y_s$ has a zero at $t = 1$, i.e., $(\exists h \in R)(f = (t - 1)h)$.

(c) It is not known whether, if the ring R contains \mathbf{Z} , the set \mathbf{Z} itself is a diophantine subset of R whenever $(\mathbf{Z}, L_{\mathbf{Z}})$ admits a diophantine model in $(R, L_{\mathbf{Z}})$.

The following result formalizes the technique of proof of many undecidability results:

Observation 3.3. Assume that R is as in 1.1, and there is a polynomial whose coefficients belong to $\phi(L)$ but that has no zero in the fraction field of R . If (M', L') has an undecidable diophantine theory, and admits a diophantine model in (R, L_R) , then the diophantine theory of (R, L_R) is undecidable. \square

Remark 3.4. Without any restrictions on R , if (M', L') has an undecidable (positive) existential theory and admits a (positive) existential model in (R, L_R) , then the (positive) existential theory of (R, L_R) is undecidable.

The technique of many undecidability proofs for rings (R, L_R) is based on the fact that, via a construction as in (3.2(b)), one can find a diophantine model of the integers $(\mathbf{Z}, L_{\mathbf{Z}})$ in (R, L_R) , and then rely on the fact that the diophantine theory

of the integers is undecidable ([13], [3]). It has been suggested that, with this more flexible definition, one would be able to find a diophantine model of the integers in the rationals:

Question 3.5. Does $(\mathbf{Z}, L_{\mathbf{Z}})$ admit a diophantine model in $(\mathbf{Q}, L_{\mathbf{Z}})$?

However, even this is impossible if we assume Mazur's conjecture:

Theorem 3.6. *Mazur's conjecture 2.1 implies that there is no diophantine model of $(\mathbf{Z}, L_{\mathbf{Z}})$ in $(\mathbf{Q}, L_{\mathbf{Z}})$.*

Proof. Assume that there is such a diophantine model (D, L_D) , with $D \subseteq \mathbf{Q}^k$. Then there is an affine variety V over \mathbf{Q} admitting a finite morphism $f : V_{\mathbf{Q}} \rightarrow \mathbf{A}_{\mathbf{Q}}^k$ defined over \mathbf{Q} such that $f(V(\mathbf{Q})) = D$.

If D is discrete (i.e., infinite and totally disconnected in the real topology), the traditional proof applies: the real topological closure of $V(\mathbf{Q})$ in $V(\mathbf{R})$ is also mapped to D by f , and hence it has infinitely many components.

If D is not discrete (which seems to be the case for the typical infinite diophantine set in \mathbf{Q} , say, the set of squares), then we show that one can select (in a computable way) a discrete subset \tilde{D} of D . Then the above proof, applied to \tilde{D} , gives the result.

Here are the details of the construction of \tilde{D} . We only have to treat the case where the real topological closure \bar{V} of $V(\mathbf{Q})$ has only finitely many connected components. Since f is continuous, the mean value theorem implies that $f(\bar{V})$ is the union of finitely many closed subsets in \mathbf{R}^k . In particular, the topological closure \bar{D} of D contains finitely many closed subsets, and since D is infinite, one of these subsets, say, D_0 , is not a point. By composing f with a suitable \mathbf{Q} -rational projection $\pi : \mathbf{A}_{\mathbf{Q}}^k \rightarrow \mathbf{A}_{\mathbf{Q}}^1$ which does not map D_0 to a point, we may assume $k = 1$. By composing with a fractional linear transformation defined over \mathbf{Q} , we may assume $\pi(D_0)$ to be the unit interval $I = [0, 1]$. Let d_n be the element of D corresponding to $n \in \mathbf{Z}$. Let us consider the set

$$\tilde{Z} = \{n \in \mathbf{Z} \mid \frac{1}{2j+1} \leq \pi(d_n) \leq \frac{1}{2j} \text{ for some } j \in \mathbf{Z}_{>0}\}.$$

The set \tilde{Z} is Turing computable (since $D = \{\pi(d_n)\}$ is a listable subset of \mathbf{Q} , it is easy to write a Turing program to check the inequalities), hence it is recursively enumerable (by Kleene's normal form theorem, cf. [23], 2.3-2.4), so by [3], it is diophantine in $(\mathbf{Z}, L_{\mathbf{Z}})$. Also, \tilde{Z} is infinite, since $\pi(D) \cap I$ is dense in I . We now set

$$\tilde{D} = \{d_n \mid n \in \tilde{Z}\}.$$

By construction, the set \tilde{D} is diophantine in (D, L_D) , and hence a fortiori in $(\mathbf{Q}, L_{\mathbf{Z}})$. So there exists a variety \tilde{V} over \mathbf{Q} and a \mathbf{Q} -morphism $\tilde{f} : \tilde{V} \rightarrow \mathbf{A}_{\mathbf{Q}}^1$ such that $\tilde{f}(\tilde{V}(\mathbf{Q})) = \tilde{D}$. However, the real closure of the set \tilde{D} has infinitely many connected components in the real topology by construction. Hence the same holds for $\tilde{V}(\mathbf{Q})$, contradicting Mazur's conjecture. \square

4. NON-ARCHIMEDEAN ASPECTS OF MAZUR'S CONJECTURES

In ([16], II.2), Mazur has devised a conjecture of the above type which applies to any completion of a number field, not just an archimedean one. As it makes sense for any global field, we formulate it as follows:

Question 4.1. Let V be a variety over a global field K , v a valuation on K , and K_v the completion of K w.r.t. v . For every point $p \in V(K_v)$, let $W(p)$ be the Zariski closure of $\bigcup(V(K) \cap U)$, where U ranges over all v -open neighbourhoods of p in $V(K_v)$. Is the set $\{W(p) : p \in V(K_v)\}$ finite?

In our next theorem, we observe that the answer to this question is negative in positive characteristic:

Theorem 4.2. *Let $K = \mathbf{F}_q(t)$ be the rational function field over a finite field \mathbf{F}_q of positive characteristic $p > 0$, and let v be the valuation corresponding to the place t^{-1} of K (i.e., $v(a) = q^{\deg(a)}$ for $a \in \mathbf{F}_q[t]$). Then there is a variety V over K for which the answer to question 4.1 is negative.*

Proof. In [19] (lemma 1) Pheidas proves that, for $p > 2$, projection onto the x -coordinate of the K -rational points of the space curve V_p given by

$$V_p : x - t = u^p - u, x^{-1} - t^{-1} = v^p - v$$

gives the set $D_p = \{t^{p^s} \mid s \in \mathbf{Z}_{\geq 0}\}$. For $p = 2$, Videla ([24]) proved that the set D_2 is the projection onto the x -coordinate of

$$V_2 : x + t = u^2 + u, u = w^2 + t, x^{-1} + t^{-1} = v^2 + v, v = s^2 + t^{-1}.$$

Already the sets $W(p)$ for $p \in V(K)$ are disjoint, since their x -coordinates are separated ($v(t^{p^s} - t^{p^r}) > 1$ for all $r \neq s$). This gives a negative answer to question 4.1. \square

Thinking of the analogy between function fields and number fields, one can ask for the strict analogue of question 3.5 for global function fields. The answer to it is *positive*:

Theorem 4.3. *For any prime power q , $q = p^n$, $p > 0$, the polynomial ring $(\mathbf{F}_q[t], L_t)$ admits a diophantine model in the ring of rational functions $(\mathbf{F}_q(t), L_t)$.*

Proof. The proof is a bit indirect: we show that the polynomial ring has a diophantine model in the positive rational integers, and the latter has a diophantine model in the field of rational functions.

More precisely, $\mathbf{F}_q[t]$ is a recursive ring (cf. Rabin [20]), because \mathbf{F}_q is recursive (since finite), and hence the same holds for the polynomial ring over \mathbf{F}_q (cf. Fröhlich and Sheperdson [7]). So there exists an injective map $\theta : \mathbf{F}_q[t] \rightarrow \mathbf{Z}_{\geq 0}$ such that the graphs of addition and multiplication are recursive on $\mathbf{Z}_{\geq 0}$, and hence $(\theta(\mathbf{F}_q[t]), \theta(L_t))$ is a diophantine model of $(\mathbf{F}_q[t], L_t)$ in $(\mathbf{Z}_{\geq 0}, L_{\mathbf{Z}})$.

For the second step, we first recall a construction of Pheidas and Videla ([19], [24]). Let v denote the t -valuation on $\mathbf{F}_q(t)$, i.e., $v(x)$ is the order of x at zero. For any $k \in \mathbf{Z}_{\geq 0}$, let $[k]$ denote the equivalence class of elements $x \in \mathbf{F}_q(t)$ with $v(x) = k$. For positive integers a and b , let $a \mid_p b$ denote the relation $(\exists n \in \mathbf{Z}_{\geq 0})(a = bp^n)$.

Consider the structure $S = (\mathbf{Z}_{\geq 0}, (+, \mid_p, 0, 1))$. Firstly, multiplication is diophantine in S ([18], corollary on p. 529). Secondly, the set of equivalence classes $[k]$ as above is a model for S in which the relations in S can be defined by diophantine formulas in $(\mathbf{F}_q(t), L_t)$ between arbitrary representatives of the equivalence classes in $\mathbf{F}_q(t)$. We conclude that for arbitrary elements $x, y, z \in \mathbf{F}_q(t)$ the relations $[v(x)] = [v(y) + v(z)]$ and $[v(x)] = [v(y) \cdot v(z)]$ are diophantine in $\mathbf{F}_q(t)$.

The problem with this encoding is that we do not know the existence of a diophantine set in $\mathbf{F}_q(t)$ which contains exactly one representative for each such equivalence class. We fix this problem as follows. We know from the proof of theorem

4.2 that the set $D_p = \{t^{p^k}, k \in \mathbf{Z}_{\geq 0}\}$ is diophantine in $(\mathbf{F}_q(t), L_t)$, and this will be our model.

To define addition and multiplication on elements of this set, we introduce the following switching between t^{p^k} and $[k]$: the set $\{(k, p^k), k \in \mathbf{Z}_{\geq 0}\}$ is recursively enumerable in $\mathbf{Z}_{\geq 0}^2$, so by Matijasevič's theorem, it is diophantine in $\mathbf{Z}_{\geq 0}$. Then, by the aforementioned results, the set $\mathcal{E} = \{([k], [p^k]), k \in \mathbf{Z}_{\geq 0}\}$ is diophantine over $(\mathbf{F}_q(t), L_t)$.

For the function symbols $R \in \{+, \cdot\}$ on $\mathbf{Z}_{\geq 0}$, we let the corresponding symbol \tilde{R} for $x, y, z \in D_p$ be defined by

$$z = x\tilde{R}y \Leftrightarrow (\exists x_1, y_1, z_1 \in \mathbf{F}_q(t))(((x_1, x), (y_1, y), (z_1, z)) \in \mathcal{E}^3 \wedge [R(x_1, y_1)] = [z_1]).$$

For $R \in \{+, \cdot\}$, the righthand side of the equivalence is diophantine in $(\mathbf{F}_q(t), L_t)$ by what we have said before and the fact that for any two elements $w_1, w_2 \in \mathbf{F}_q(t)$, the statement $[w_1] = [w_2]$ is equivalent with $(v(w_1/w_2) \geq 0) \wedge (v(w_2/w_1) \geq 0)$, which is diophantine by [19] and [24].

Finally, $(D_p, \tilde{+}, \tilde{\cdot}, t, t^p)$ is a diophantine model of $(\mathbf{Z}, L_{\mathbf{Z}})$ in $(\mathbf{F}_q(t), L_t)$. This finishes the proof of the theorem. \square

Of course, the above theorem still does not settle the following problem:

Question 4.4. Is the polynomial ring $\mathbf{F}_q[t]$ a diophantine subset of the field of rational functions $\mathbf{F}_q(t)$?

REFERENCES

1. J.-L. Colliot-Thélène, A. N. Skorobogatov, and P. Swinnerton-Dyer, *Double fibres and double covers: paucity of rational points*, Acta Arith. **79** (1997), no. 2, 113–135.
2. G. Cornelissen, *Stockage diophantien et hypothèse abc généralisée*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 1, 3–8.
3. M. Davis, Y. Matijasevič and J. Robinson, *Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution*. in: Mathematical developments arising from Hilbert problems (Northern Illinois Univ., De Kalb, Ill., 1974), Proc. Sympos. Pure Math. **XXVIII**, pp. 323–378, Amer. Math. Soc., Providence, R. I., 1976
4. J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.
5. J. Denef, *p-adic semi-algebraic sets and cell decomposition*, J. Reine Angew. Math. **369** (1986), 154–166.
6. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366 (Erratum: Invent. Math. **75** (1984), 381).
7. A. Fröhlich and J.C. Shepherdson, *Effective procedures in field theory*, Philos. Trans. Roy. Soc. London Ser. A. **248** (1956), 407–432.
8. J.G Hocking and G.S. Young, *Topology*, Dover Publications, New York, 1988, 2nd edition.
9. W. Hodges, *A shorter model theory*, Cambridge Univ. Press, Cambridge, 1997.
10. L. Lipshitz, *The Diophantine problem for addition and divisibility*, Trans. Amer. Math. Soc. **235** (1978), 271–283.
11. L. Lipshitz, *Some remarks on the Diophantine problem for addition and divisibility*, in: Proceedings of the Model Theory Meeting (Univ. Brussels, Brussels/Univ. Mons, Mons, 1980), Bull. Soc. Math. Belg. Sr. B **33** (1981), 41–52.
12. A. Macintyre, *On definable subsets of p-adic fields*, J. Symbolic Logic **41** (1976), no. 3, 605–610.
13. Ju. V. Matijasevič, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282.
14. B. Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45.
15. B. Mazur, *Speculations about the topology of rational points: an update*, in: Columbia University Number Theory Seminar (New York, 1992), Astérisque **228**, pp. 165–182, 1995.

16. B. Mazur, *Open problems regarding rational points on curves and varieties*, in: Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser. **254**, pp. 239–265, Cambridge Univ. Press, Cambridge, 1998.
17. J. Milnor, *On the Betti numbers of real varieties*, Proc. Amer. Math. Soc. **15** (1964), 275–280.
18. T. Pheidas, *An undecidability result for power series rings of positive characteristic. II.*, Proc. Amer. Math. Soc. **100** (1987), no. 3, 526–530.
19. T. Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), no. 1, 1–8.
20. M.O. Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360.
21. J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114 (=Collected works (eds. S. Feferman), Amer. Math. Soc., Providence, 1996, pp. 7–23).
22. J.H. Silverman, *Advanced topics in the Arithmetic of Elliptic curves*, Graduate Texts in Math. textbf151, Springer Verlag, Berlin, 1995.
23. R. I. Soare, *Recursively enumerable sets and degrees*, Springer-Verlag, Berlin, 1987.
24. C. Videla, *Hilbert's tenth problem for rational function fields in characteristic 2*, Proc. Amer. Math. Soc. **120** (1994), 249–253.

GHENT UNIVERSITY, DEPARTMENT OF PURE MATHEMATICS AND COMPUTER ALGEBRA, GAL-
GLAAN 2, B-9000 GENT

Current address: Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn

E-mail address: `gc@cage.rug.ac.be`

GHENT UNIVERSITY, DEPARTMENT OF APPLIED MATHEMATICS AND COMPUTER SCIENCE, KRI-
JGSLAAN 281, B-9000 GENT

E-mail address: `karim.zahidi@rug.ac.be`